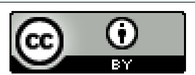
Bokareva, A.A., & Tagiltseva, E.A. (2022). Creation of architecture and development of a mobile application Unified Personal Medical Card. *Actual Issues of Modern Science. European Scientific e-Journal*, *4*(19), 29-37. Ostrava: Tuculart Edition. (in Russian)
Бокарева, А.А., Тагильцева, Е.А. (2022). Создание архитектуры и разработка мобильного приложения Единая Персональная Медицинская Карта. *Actual Issues of Modern Science. European Scientific e-Journal*, *4*(19), 29-37. Ostrava: Tuculart Edition.

DOI: 10.47451/inn2022-03-02

The paper will be published in Crossref, ICI Copernicus, J-Gate, ISI, Academic Resource Index ResearchBib, Internet Archive, Google Scholar, eLibrary, Ukrainian National Library databases.



Alyona A. Bokareva, Researcher in the field of electronic documentary, Undergraduate, ITMO University, St Petersburg, Russia. ORCID: 0000-0003-1174-3574.
Elizaveta A. Tagiltseva, Researcher in the field of electronic documentary, Undergraduate, ITMO University, St Petersburg, Russia. ORCID: 0000-0002-6954-1644.

Creation of architecture and development of a mobile application Unified Personal Medical Card

Abstract: The article is devoted to the development of the architecture and creation of the mobile application Unified Personal Medical Card, which allows you to completely replace the paper version of standardized cards of medical institutions, provide the user with the opportunity to have access to their medical data at any time, simplify the work of emergency medical services and reduce the costs of compulsory medical insurance funds. The article reflects aspects of access protection and the possibility of combining with a single electronic document of a citizen, which in the future will allow switching to an electronic format of interaction with any government agencies within the framework of working with one application. Social surveys were used as methods for determining social significance and the current market of mobile applications was studied to identify analogues and their shortcomings in functioning. MySql, Figma and UML diagrams were used to form the architecture. The research existing proposals and opportunities reflected in the list of sources of information.

Keywords: mobile application, development, personal data, electronic document, identification, authentication, medical data.



Алёна Александровна Бокарева, исследователь в области электронной документации, магистрант, Университет ИТМО, Санкт-Петербург, Россия.
Елизавета Анатольевна Тагильцева, исследователь в области электронной документации, магистрант, Университет ИТМО, Санкт-Петербург, Россия.

Создание архитектуры и разработка мобильного приложения Единая Персональная Медицинская Карта

Аннотация: Статья посвящена разработке архитектуры и созданию мобильного приложения Единая Персональная Медицинская Карта, позволяющему полностью заменить бумажный вариант стандартизированных карт медицинских учреждений, предоставить пользователю возможность иметь доступ к своим медицинским данным в любой необходимый момент, упростить работу экстренных медицинских служб и сократить расходы фондов обязательного медицинского страхования. В статье отражены аспекты защиты доступа и возможности объединения с единым электронным документом гражданина, что в будущем позволит перейти

на электронный формат взаимодействия с любыми государственными структурами в рамках работы с одним приложением. В качестве методов определения социальной значимости были использованы социальные опросы и изучен текущий рынок мобильных приложений на предмет выявления аналогов и их недостатков функционирования. Для формирования архитектуры были использованы MySql, Figma и UML диаграммы. В ходе исследования были изучены существующие предложения и возможности, отраженные в списке источников информации.

Ключевые слова: мобильное приложение, разработка, персональные данные, электронный документ, идентификации, аутентификация, медицинские данные.



Вступление

В условиях перехода на электронный документооборот, высокой скорости общего ритма жизни и повышения мобильности возрастает необходимость в предоставлении актуальной информации о состоянии здоровья с сохранением истории проведенных обследований и их результатов для пользователя в максимально удобном и доступном формате. Данное направление является приоритетным для развития социального программного обеспечения и дает возможность для сокращения затрат государства на обеспечение здравоохранения.

Каждый имеет право получить в доступной для него форме имеющуюся в медицинской организации информацию о состоянии своего здоровья, в том числе сведения о результатах медицинского обследования, наличии заболевания, об установленном диагнозе и о прогнозе развития заболевания, методах оказания медицинской помощи, связанном с ними риске, возможных видах медицинского вмешательства, его последствиях и результатах оказания медицинской помощи (*Федеральный закон № 317-ФЗ*).

Исходя из описанной проблематики была выявлена потребность в создании универсального мобильного приложения для работы с персональной медицинской информацией в условиях распределенных серверов первоначального ее хранения и обеспечения безопасности работы за счет использования дополнительных функций защиты доступа.

Целью данного исследования является определение основных параметров приложения для работы с персональной медицинской информацией и определение методов обеспечения конфиденциальности при работе с ней.

Детальное рассмотрение целей позволяет сформулировать задачи для данного исследования. Основными задачами будут являться: корректная обработка информации, полученной с распределенных серверов лечебно-профилактических учреждений, имеющая различный формат и тип данных; защита персональной медицинской информации и предотвращение несанкционированного доступа и потери данных. Необходимо определить потенциальных пользователей, их социальный и возрастной статус, провести анализ конкурентоспособности и жизнеспособности приложения, а также его востребованность на рынке. Разработка интуитивно понятного интерфейса для работы с приложением исходя из выделенной социальной и возрастной группы

пользователей является одной из немаловажных задач.

Методы, использованные в исследовании

На текущий момент первые шаги в рамках предоставления оперативного доступа к персональной медицинской информации осуществляются путем введения на портале ГосУслуг для жителей Москвы и Санкт-Петербурга (например, Электронный ресурс «Здоровье Петербуржца»), где отражены основные данные по совершенным визитам к специалистам, назначениям и диагнозам в рамках данных визитов и результаты различных лабораторных и инструментальных исследований. Однако все приведенные сведения касаются только территории прикрепления полиса ОМС, что не позволяет получить полную картину для проведения какого-либо статистического или аналитического анализа.

В рамках работы по созданию данного мобильного приложения были определены стадии и необходимые шаги по реализации и внедрению данной разработки в рамках города и страны. С учетом Федеральных законов о защите персональных данных и децентрализованности серверов различных лечебно-профилактических учреждений даже в пределах одной территории для полноценной реализации и внедрения данного продукта даже на этапе тестирования и создания минимально жизнеспособного приложения (MVP) необходима поддержка и заинтересованность со стороны Правительства и Министерства Здравоохранения, что существенно снижает скорость разработки приложения. Однако коммерческая ценность продукта и оптимизированный переход на электронные документы позволяют сделать вывод о реализуемости и значимости данной разработки на сегодняшний день.

Конкурентные приложения не имеют алгоритмов для сбора данных с различных распределенных ресурсов и алгоритмов обработки данных разного формата для приведения их в единую форму для анализа и восприятия, что позволяет говорить о низком уровне конкуренции на текущий момент.

Оптимальным вариантом выбора для разрешения задачи эффективного доступа к медицинским данным является создание мобильного приложения, позволяющего автоматически загружать с распределенных серверов медицинских учреждений всю хранящуюся там информацию о владельце данного приложения с использованием систем идентификации и аутентификации, в том числе и с возможностью использования биометрических систем. Использование биометрических параметров в качестве и ключа и метода криптографической защиты является оптимальным вариантом для решения поставленной задачи. Если представить считанные биометрические данные в виде координатной сетки, то сам процесс верификации документа и аутентификации личности может быть организован через некоторую предопределенную функцию изменения характеристик (цифрового кода) точки, определенный координатной сеткой биометрических параметров (в дальнейшем – карта изменения). Соответственно, при считывании биометрических параметров мы получаем: карту изменений (координаты точек, которые должны быть модифицированы для верификации и аутентификации), ключ к самому алгоритму изменения точек и низкую вероятность отказов 1 и 2 типа (*Bokareva, 2020a*). Данный алгоритм может быть использован как основной для

аутентификации и идентификации пользователя в условиях доступа к данным приложения без использования передачи данных, что позволяет работать и в условиях отсутствия доступа в сеть Интернет.

В результате создания мобильного приложения Единая Персональная Медицинская Карта (далее – ЕПМК) пользователь сможет оперативно получить информацию о проведенных медицинских манипуляциях в любой точке мира, что позволит: проводить плановые и экстренные мероприятия по оказанию медицинской помощи, основываясь на истории болезни человека в любом медицинском учреждении и стационаре без дополнительных затрат ресурсов (в том числе и временных) на сбор анамнеза; сократить количество ошибок, полученных за счет искажения при сборе информации и результата прошлых обследований от пациента; сократить затраты на обращение в медицинские учреждения за результатами анализов; получить возможность консультаций в других медицинских учреждениях на основании ранее сделанных обследований состояния здоровья; проводить анализ основных показателей и оповещать о необходимости посещения врача; оповещать население о чрезвычайных ситуациях и изменениях санитарных и профилактических мер с использованием функций всплывающих окон; проводить научные и медицинские исследования на основании масштабной базы данных, при наличии согласия пользователя к использованию деперсонализированной информации о проведенных исследованиях и перенесенных заболеваниях.

Для реализации приложения ЕПМК необходимо создание архитектуры программного обеспечения и разработка дизайна, отвечающего современным стандартам и требованиям со стороны пользователя. Основная сложность в работе с получаемыми медицинскими данными состоит в разнородности информации и огромному количеству форматов даже внутри одного территориального звена или медицинского учреждения. Работа по приведению к единому стандарту и анализу получаемой информации должна проводиться в самом приложении и использовать быстро действенные алгоритмы. Для формирования данных алгоритмов и проверки их эффективности была использована тестовая база данных из реальных пакетов данных об исследованиях разработчиков проекта. В ходе проведения анализа получаемых данных было установлено, что основная часть приходит в едином формате и различаются лишь незначительная часть документов, чаще всего в значениях референсных норм и единиц измерения. Создание оптимального алгоритма свелось к стандартной задаче, что существенно упростило работу по построению внутренней архитектуры приложения. Также необходимо построение аналитических кривых по основным показателям (например, анализа крови), выведение результата и рекомендаций.

В процессе создания архитектуры ЕПМК возникла необходимость добавить в функционал возможность получения назначений и отслеживания графика приема лекарственных средств, что, в свою очередь, так же является необходимой информацией не только для пользователя в формате удобства, но и для медицинских работников, в частности служб экстренной помощи, при необходимости принятия решения в короткие сроки и понимания возможных последствий, в том числе от взаимодействия лекарственных средств между собой.

Была разработана и построена база данных, оперирующая основными данными о

пользователе. В качестве основного определяющего параметра был выбран страховой номер индивидуального лицевого счёта (СНИЛС). СНИЛС – страховой номер индивидуального лицевого счета - уникальный номер индивидуального лицевого счета, используемый для обработки сведений о физическом лице в системе индивидуального (персонифицированного) учета, а также для идентификации и аутентификации сведений о физическом лице при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций (*Федеральный закон №27-ФЗ*). На индивидуальный лицевой счёт заносятся все данные о начисленных и уплаченных работодателем страховых взносах в течение всей трудовой деятельности гражданина, которые впоследствии учитываются при назначении или перерасчёте пенсии. Присвоение страхового номера носит технологический характер и осуществляется в целях упрощения порядка и ускорения процедуры назначения трудовых пенсий застрахованным лицам.

СНИЛС есть у всех работающих граждан – большинство россиян (за исключением военнослужащих) получают его на первом месте работы, однако, возможно и его самостоятельное оформление на себя или на своего несовершеннолетнего ребёнка.

Формат СНИЛС: «XXX-XXX-XXX YY», где X, Y – цифры, причём первые девять цифр 'X' – это любые цифры, а последние две 'Y' фактически являются контрольной суммой, вычисляемой по особому алгоритму из последовательности первых 9 цифр (*Федеральный закон №27-ФЗ*). СНИЛС является одним из немногих документов для граждан России, идентификационные данные которого не меняются в течение всей жизни индивида и наиболее точно подходит под требования идентификации пользователя в распределенных базах данных медицинских учреждений, поскольку имеет привязку ко всем анализам и обследованиям гражданина. С 2012 года СНИЛС выдается также не гражданам России, приехавшим по рабочей визе, что расширяет возможности использования приложения не только гражданами.

При разработке также было решено отказаться от идентификатора «врач», который создавал избыточность в таблице, не внося существенно важных значений. Использование идентификатора медицинского учреждения как основного для документации и поиска нужной информации о постановке диагноза или назначении препарата является достаточным в данном решении.

В качестве протокола передачи данных должен использоваться HTTPS (HyperText Transfer Protocol Secure), являющийся на данный момент стандартом передачи произвольных данных. Вся информация, может быть зашифрована, что необходимо при работе с медицинскими данными, являющимися персональными данными. В качестве метода шифрования в разработке архитектуры ЕПМК был выбран победитель конкурса AES, наиболее стойкий и быстрый алгоритм блочного шифрования Rijndael, позже взявший название конкурса. Размер ключа однозначно должен быть 128 бит, так как это максимально допустимый размер для ассиметричный методов шифрования на территории Российской Федерации (*Алгоритмы шифрования*).

В медицинской сфере достоверность переданных и полученных данных является крайне важным критерием, даже незначительные ошибки могут привести к потере здоровья или снижению качества жизни. Выбранный HTTPS протокол с проверкой

сертификата и надежным механизмом шифрования полностью гарантирует защиту и целостность доставленных пакетов. В случае обнаружения поврежденного пакета запрос будет передан повторно.

При разработке приложения ЕПМК для комфортного использования со стороны пользователя были определены следующие характеристики: простая и пошаговая регистрация; создание красивого и понятного пользовательского интерфейса; проработка удобного и понятного для любого пользователя функционала приложения; простая взаимосвязь и обмен информации между пользователем и медицинским учреждением; возможность использовать приложение на ходу (используя мобильный трафик); добавление определений ко всем терминам, упомянутых в приложении.

При условии сочетания разработанного мобильного приложения и систем идентификации и аутентификации с использованием биометрических параметров можно получить безопасный (с точки зрения доступа и хранения персональных данных) инструмент для оказания экстренной и плановой помощи населению.

Экономические расчеты показали, что снижение затрат при подключении к использованию ЕПМК составляют от 47% до 68% по истечению 5 лет использования, что, в масштабах выделяемых средств на фонды обязательного медицинского страхования дает принципиально новые возможности для развития текущей системы здравоохранения, замены оборудования и построения новых медицинских учреждений. Процентный показатель варьируется исходя из понимания минимального и максимального количества возможных подключений, зависящий как от территориальных показателей (для России характерно неравномерное распределение населения и ресурсов, в том числе технических), так и от активной возрастной группы.

В дальнейшем данное приложение имеет возможность подключиться к Единого Электронного Документа Гражданина (далее – ЕЭДГ), что позволит окончательно завершить цифровую революцию перехода с бумажных носителей на электронные.

Единый Электронный Документ Гражданина – это документ, идентифицирующий личность предъявителя должен обладать исчерпывающими, но не перенасыщенными по содержанию данными о персоне. На сегодняшний день подобными данными являются фамилия, имя, отчество (при наличии), дата рождения и уникальный номер, присвоенный какому-либо документу (не персоне), удостоверяющему личность и при выдаче нового документа (или нового типа документа, например, водительское удостоверение) присваивается новый номер, что в свою очередь приводит к прогрессирующим объемам хранимой информации о каждом идентифицируемом человеке. При переходе на электронный документооборот целесообразна замена всех имеющихся идентификаторов (номеров документов) на единый уникальный номер, присваиваемый персоне, а не конкретному документу. А всеобщий массив данных (паспорт, водительское удостоверение, СНИЛС, полис и т.д.) в свою очередь необходимо и достаточно заменить единым электронным документом с прописанными и полностью объединенными в общую базу данных социально-юридические характеристики конкретного человека (идентифицируемой персоны). Данная система позволит одновременно сохранить всю значимую информацию в одном «файле», будет препятствовать размножению различных форм и количества документов (и их идентифицирующих номеров, нуждающихся в

последующем хранении), увеличивающих риск потери и искажения. Так же данная система обеспечит удобство использования и комфорт, как для пользователя, так и для различных государственных и иных заинтересованных структур, за счет возможности использования вне зон устойчивой связи, без ношения дополнительных устройств и бланков (для пользователя), высокая степень надежности и быстродействия, обеспечивающая минимальные отказы по первому и второму типу ошибок (*Алгоритмы шифрования*; *Абрамова, 2020*). Согласно требованию законодательства Российской Федерации допустимо использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз (*Постановление Правительства РФ № 1119*; *Емельянов и Носова, 2019*), что приводит к необходимости провести тестирование и последующую оценку разработанного алгоритма (*Железняк и др., 2018*).

Использование ЕЭДГ в совокупности с разрабатываемым мобильным приложением ЕПМК позволяет убрать избыточные хранимые данные за счёт уже пройденной идентификации и аутентификации при входе в само приложение, соотносить персональные данные человека с его медицинской информацией, оказывать медицинские услуги на месте, без необходимости установки личности. Однако, при использовании биометрических данных в качестве основной системы безопасности возникают риски, в которых пациент может не получить необходимую помощь ввиду отсутствия возможности «предъявить» биометрические параметры пользователя. Данный аспект требует дополнительной проработки и создания безопасной системы альтернативного входа для сотрудников экстренных служб медицинской помощи. Его реализация должна гарантировать отсутствие несанкционированного доступа к данным в любой штатной ситуации и предотвратить утечку информации, представляющей собой медицинскую тайну (*Саушкин, 2020*).

На текущий момент разработка интерфейса мобильного приложения ЕПМК полностью реализована, тестирование завершено и по окончании доработки баз данных приложение может быть выпущено на рынок, как полноценная замена существующих бумажных медицинских карт.

Дискуссия

В рамках дальнейшей работы необходима детальная разработка и оценка эффективности предложенного метода аутентификации и идентификации для доступа к персональной медицинской информацией и соответствие его текущим требованиям законодательства в отношении защиты и обработки персональных данных (в частности – медицинских данных). Отказоустойчивость приложения, выбранный метод хранения и обработки данных требуют тщательного тестирования во избежание утери и повреждения персональных данных с учетом специфики работы данного приложения (в рамках оказания экстренной медицинской помощи). Немаловажным аспектом разработки является создание дополнительного канала доступа к данным в условиях чрезвычайных ситуаций, не позволяющих реализовать вход с использованием биометрических параметров владельца для экстренных служб согласно протоколу разрешенного доступа

к информации (сотрудники службы скорой медицинской помощи, спасатели и иные лица, имеющие законодательное разрешение к доступу к персональным медицинским данным).

Заключение

Таким образом, необходимо отметить, что разрабатываемое мобильное приложение имеет важное стратегическое, социальное и экономическое значения не только для отдельных пользователей, но и для всей системы здравоохранения в целом. Объединение мобильного приложения ЕПМК и документа ЕЭДГ позволит создать абсолютно независимую систему аутентификации и идентификации пользователя и способна заменить все существующие бумажные документы пользователя, сделав коммуникацию с государственными институтами простой, доступной и прозрачной, а затраты государства на выпуск, хранение и сбор данных о гражданах свести к минимальному обслуживанию серверов и баз данных.

Несмотря на очевидность эффективности практического применения данных методов и разработок в современном цифровом государстве, необходимо оценить экономические аспекты внедрения, перспективы использования среди различных групп населения (в том числе, людей старшего возраста), риски утери или искажения данных и резервные варианты доступа к персональным данным, в том числе алгоритмы получения разрешения и динамический ключ доступа.



Список источников информации:

Абрамова, А.Г. (2020). Современные проблемы осуществления защиты персональных данных в сети: основополагающие принципы защиты персональных данных. *Регион и мир*, *4*(11), 21-25.

Алгоритмы шифрования. Финалисты конкурса AES. Часть 2. Обращение 10 декабря 2021 года к https://www.ixbt.com/soft/alg-encryption-aes-2.shtml

Емельянов, Е.Г., Носова, Ж.Е. (2019). Методика сбора персональных данных пользователя в мобильных приложениях в соответствии с федеральным законом «О персональных данных». *Сборник материалов 3-й Всероссийской конференции, посвященной 55-летию ЮЗГУ. Программная инженерия: современные тенденции развития и применения*, 289-292.

Железняк, В.П., Ряполов, К.Я., Вялых, С.А., Чапурин, Е.Ю. (2018). Определение актуальных угроз безопасности персональных данных в информационных системах персональных данных. *Сборник материалов Всероссийской научно-практической конференции. Актуальные проблемы деятельности подразделений УИС*, 88-91.

Петров, М.И. (2007). *Комментарий к федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ: (постатейный)*. Серия «Библиотека журнала «Право и экономика». Москва: Юстицинформ.

Постановление Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах

персональных данных». Обращение 10 декабря 2021 года к http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/

Саушкин, С.О. (2020). Понятие института защиты персональных данных при автоматизированной обработке персональных данных. *Научный электронный журнал Меридиан*, *7*(41), 216-218.

Федеральный закон №27-ФЗ от 01.04.1996 «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (последняя редакция). Обращение 1 декабря 2021 года к http://www.consultant.ru/document/cons_doc_LAW_9839/#dst100406

Федеральный закон № 317-ФЗ, ст. 22. от 25.11.2013 «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации по вопросам охраны здоровья граждан в Российской Федерации» Обращение 10 декабря 2021 года к http://www.consultant.ru/document/cons_doc_LAW_154744/

Bokareva, A.A. (2020a). Model of a document protection algorithm for a person based on biometric parameters. *Actual Issues of Modern Science. European Scientific e-Journal*, *6* (6), 1, 12-19. Hlučín-Bobrovníky: “Anisiia Tomanek” OSVČ. (англ.) DOI: 10.47451/inn2020-09-002.

Bokareva, A.A. (2020b). Personal authentication using verified electronic document. *Actual Issues of Modern Science. European Scientific e-Journal*, *6* (6), 1, 5-11. Hlučín-Bobrovníky: “Anisiia Tomanek” OSVČ. (англ.) DOI: 10.47451/inn2020-09-001.